論文の内容の要旨

論文題目 On The Security Of Multiple Encryptions

（多重暗号化の安全性に関する研究）

氏名　張　鋭

（本文）暗号の第一義的な意味は、誰もが盗聴することができる公開通信路上における守秘通信を実現することにある。しかしながら、盗聴者自身がシステムの正規のユーザである場合など、状況によっては、受動的な盗聴に対してだけでなく、能動的なより強力な攻撃を想定しなければならない。このようなより一般的な状況を議論する現代暗号にとって要求される安全性が、攻撃者が選択暗号文攻撃に対する安全性である、という認識が確立するまでに20年以上の歳月が必要であった。さらに、このような安全性を持つ暗号の構成法については、最近まで知られていなかった。

本論文では、より一般的なシナリオとして、多重暗号を議論する。多重暗号とは、簡単に言えば、いくつかの暗号を一つのメッセージを暗号化する方法であり、それぞれの暗号は全体に対する部品として考えることができる。部品が一つの場合、即ちたった一つの暗号による多重暗号を考える場合は、従来の伝統的な暗号であると考えることができるため、その意味において、多重暗号は従来の暗号を含んでいる。

多重暗号の安全性については、限定された場合については、すでに研究が行われており、そこでは多重暗号により安全性が強められるか、もしくは、少なくとも部品中の特定の暗号と同じ程度安全である、というある意味で直感的な結論が示されている。しかし本論文では、この結論が必ずしも正しくなく、鍵漏洩と選択平文攻撃を考えた場合には、多重暗号の結果、それを構成しているどの暗号の安全性よりも低下することがあることを指摘する。

多重暗号は、いくつかの標準化委員会において、安全性を高めるための方法として推奨されているだけでなく、ミックスネットなどのプロトコル実現のためのきわめて有効な構成要素として利用されてきた事情があり、われわれの結果

の持つ意味は極めて大きい。これにより、安全な多重暗号が存在するのか、さらに、もし存在するとすれば、どのようにそれを実現できるのか、という問題が極めて現実的な意味を持つことになるからである。

本論文では、上記の二つの問題に対する肯定的な解答が与えられる。即ち、安全な多重暗号が存在すること、および、安全な多重暗号のいくつかの具体的な構成方法が示される。特に、多重暗号のモデルを定式化し、多重暗号のための安全性の概念を理論的に整備した。

モデルの定式化については、まずは、ランダムオラクルを仮定した定式化を行い、その後ランダムオラクルの存在を仮定しないスタンダードモデルにおいても可能なことを示した。

安全性の概念の理論的整備については、我々は、さまざまな安全性概念の間の関係について分析すると同時に、安全性証明に必要な概念を簡単な工学的操作により扱うことができる方法を指摘する。

また、単一鍵による多重暗号についても研究を行った。これは、復号サーバが、構成暗号すべてについてたった一つの鍵を知っている状況である。この研究には、（IDに基づく）暗号の安全性を解くことが難しいとされる他の数学的問題へタイトに帰着する際に必要な、重要なテクニックを与えるという応用がある。また、匿名の鍵更新方式の安全性を証明する際にも同様のテクニックを用いることができる。

さらに、我々はAll-or-Nothing と呼ばれるある種の秘密分散方式を用いた暗号システムの安全性について解析を与えた。この解析は、パラレルな多重暗号、あるいはそれと類似の方式と密接な関係があるが、従来研究では、このような暗号システムの安全性については不明瞭であり、我々の研究はその意味においても大きな貢献であると自負している。